UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,812	12/27/2001	Eric J. Sprunk		7975

20350 7590 02/02/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 02/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/049,812	SPRUNK ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 10-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 10-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 and 10-19 are pending in this office action.

2. Applicant's arguments, filed November 23, 2005, have been fully considered but they are not persuasive.

Claim Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 16-19 rejected under 35 U.S.C. 102(b) as being anticipated by Lewis (U.S. Patent No. 5,761,306).

Regarding claim 16, Lewis teaches a method of updating a cryptographic key used for decrypting distributed data, the method comprising:

- Generating a first key for decrypting the distributed data, the first key of a first length (fig. 2, ref. num S1 and col. 5, lines 50-55);
- Encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length (col. 9, lines 26-32); and
- Distributing the encrypted first key (fig. 6, ref. num S8 and S9A).

Regarding claim 17, Lewis teaches further comprising distributing data encrypted with the first key (col. 1, lines 41-60).

Regarding claim 18, Lewis teaches further comprising:

- Generating a third key to replace the first key, the third key of a third length, wherein the third length is shorter than the second length (col. 11, lines 39-49);
- Encrypting the third key with the second key (col. 10, lines 17-24); and
- Distributing the encrypted third key (col. 11, lines 50-56).

Regarding claim 19, Lewis teaches further comprising distributing data encrypted with the third key (col. 1, lines 41-60).

Claim Rejections - 35 USC § 103

6. Claims 1-7 and 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (USP '306) in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, pps. 183-184 (hereinafter Schneier).

Regarding claim 1, Lewis teaches an asymmetric cryptographic processing system using a multiple key hierarchy, the asymmetric cryptographic processing system comprising:

- A first key for performing asymmetric operations at a first rate, wherein each operation requires a first cryptographic processing time (fig. 2, ref. num S1 and col. 5, lines 50-55); and
- A second key for performing an asymmetric cryptographic processing operation to update the first key (fig. 2, ref. num S2 and col. 5, lines 50-55), wherein the second key is used for cryptographic processing operations **for the first key** (col. 9, lines 26-32) and requires a second cryptographic processing time greater than the first cryptographic processing time (col. 7, lines 43-50).

Lewis does not teach wherein the second key is at a second rate that is less often than the first rate.

Schneier teaches wherein the second key is at a second rate that is less often than the first rate (section 8.10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the second key processes at a second rate that is less than the first rate, as taught by Schneier, with the method/medium of Lewis. It would have been obvious for such modifications because different keys are used differently for

different applications. Telephone communication keys should be changed with every call, whereas keys for storage of files should rarely be changed (see section 8.10 of Schneier). If the second key requires more processing time, as claimed above, it would be beneficial to change the rate of the key less than that of the first key.

Regarding claims 2-5, Lewis as modified by Schneier teaches wherein the system is used to cryptographically process and transfer digital [voice/audio/video] data in a network (see col. 1, lines 41-60 of Lewis).

Regarding claim 6, Lewis as modified by Schneier teaches wherein the second key is hard coded into the system at the time of manufacturing the system (see section 8.10 of Schneier and col. 7, lines 43-50 of Lewis, it would provide more security if the second key were hard coded into the system in a case where the second key was used for a more intensive cryptographic process and changed less often).

Regarding claim 7, Lewis as modified by Schneier teaches wherein a plurality of digital cryptographic processing systems are coupled by a telecommunications system, wherein the second key is distributed to two or more of the asymmetric cryptographic processing systems via the telecommunications system (fig. 1, ref. num 10/12/16/26 of Lewis).

Regarding claim 10, Lewis teaches a method for providing secure data transactions in a telecommunications system, wherein a digital processing device receives information from the telecommunications system (abstract), wherein the digital processing device uses a first asymmetrical cryptographically processed key to perform an asymmetric cryptographic processing operation to decode the information wherein the cryptographic processing operation is at a first level of complexity requiring a first amount of resources by the processing device (fig. 2, ref. num S1/S2), wherein the cryptographic processing operation is performed at a first rate of cryptographic processing operations per unit time (col. 5, lines 50-55), the method comprising:

- Transferring a second asymmetrical cryptographically processed key to the digital processing device (fig. 2, ref. num S8), wherein the second asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a second level of complexity requiring a second amount of resources by the processing device that is higher than the first amount of resources (col. 7, lines 43-50);
- Updating the first asymmetrical cryptographically processed key from time-to-time (fig. 2, ref. num S8-S10), wherein the updating includes the following substeps;
- Encoding a substitute first asymmetrical cryptographically processed key with a second key (col. 8, lines 15-27), so that the resulting cryptographically processed substitute first asymmetrical cryptographically processed key is decodable by the second asymmetrical cryptographically processed key (col. 10, lines 17-24); and

- Transferring the substitute first asymmetrical cryptographically processed key to the digital processing device so that the substitute first asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device (col. 10, lines 30-49).

Lewis does not teach wherein the updating of the first asymmetrical cryptographically processed key occurs at a second rate of cryptographic processing operations per unit time that is less than the first rate of cryptographic processing operations per unit time.

Schneier teaches wherein the updating of the first asymmetrical cryptographically processed key occurs at a second rate of cryptographic processing operations per unit time that is less than the first rate of cryptographic processing operations per unit time (section 8.10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine transferring replacement keys to the devices at a second rate that is less than the first rate, as taught by Schneier, with the method/medium of Lewis. It would have been obvious for such modifications because different keys are used differently for different applications. Telephone communication keys should be changed with every call, whereas keys for storage of files should rarely be changed (see section 8.10 of Schneier). If the second key requires more processing

time, as claimed above, it would be beneficial to change the rate of the key less than that of the first key.

Regarding claim 11, Lewis as modified by Schneier teaches further comprising:

- Transferring a third asymmetrical cryptographically processed key to the digital processing device (see fig. 2, ref. num S10 of Lewis), wherein the third asymmetrical cryptographically processed key is used in an asymmetric cryptographic processing operation at a third level of complexity requiring a third amount of resources by the processing device that is higher than the second amount of resources (see col. 7, lines 43-50 of Lewis);
- Updating the second asymmetrical cryptographically processed key from time-to-time (see fig. 2, ref. num S8-S10 of Lewis), wherein the updating of the second asymmetrical cryptographically processed key occurs at a third rate of cryptographic processing operations per unit time that is less than the second rate of cryptographic processing operations per unit time (see section 8.10 of Schneier), wherein the updating includes the following substeps;
- Encoding a substitute second asymmetrical cryptographically processed key with a third asymmetrical cryptographically processed key (see col. 8, lines 15-27 of Lewis), so that the resulting cryptographically processed substitute second asymmetrical cryptographically processed key is capable of being cryptographically processed by the third asymmetrical cryptographically processed key (see col. 10, lines 17-24 of Lewis); and

- Transferring the substitute second asymmetrical cryptographically processed key to the digital processing device so that the substitute second asymmetrical cryptographically processed key is used in subsequent cryptographic processing operations by the digital processing device (see col. 10, lines 30-49 of Lewis).

Regarding claims 12-15, Lewis as modified by Schneier teaches wherein the resources include [processing time/transistor density on an IC/memory capacity/data bandwidth] (see section 8.10, page 184 of Schneier and col. 7, lines 43-48 of Lewis).

Response to Arguments

7. Applicant amends claim 1.

8. Applicant argues: Neither Lewis or Schneier discloses the second key, used in cryptographic processing operations of the first key, needing a second cryptographic processing time greater than the first cryptographic processing time to process the first key (page 10, first paragraph).

Regarding applicant's argument, examiner disagrees with applicant. Applicant amended claim 1 to state that the second key was used in cryptographic processing operations **on the first key** at a second rate. Prior to this amendment, the claim stated that the second key is used in cryptographic processing operations at a second rate. Lewis clearly states that a second key (replacement key) is used in cryptographic processing operations at a second rate and at a greater length (see col. 7, lines 43-48

of Lewis). Lewis states that the replacement key is longer than the key it is replacing. One of ordinary skill in the art knows that the longer the key, the more secure it is because it takes more time (resources and processing time) to discover the key.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

Primary Examiner
AU2131
1/31/06